UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,086	03/11/2004	Nobuyuki Osaki	16869B-105700US	8546

20350 7590 08/22/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 08/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/799,086	OSAKI, NOBUYUKI	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,9-25 and 27-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,9-25 and 27-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/31/05 & 3/11/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 6, 9-17, 20-23, 25, 27-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Bojinov et al. (U.S. Pub. No. 2005/0102498).

Referring to claim 1:

Bojinov et al. teach:

A method for encrypted data storage in a storage system, the method comprising:

Converting blocks of data to produce corresponding converted blocks of data, wherein a converted block of data is encrypted with cryptographic criteria (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.);

Receiving a read request to access the read data from the storage system, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.).

Referring to claim 2:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose that the conversion replaces each block of data by a corresponding converted block of data thereof (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 3:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose that the steps of encryption and decryption comprise executing computer program code on a data processing component (see claims 26, 28 of Bojinov et al.).

Referring to claim 4:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose a communication network comprising a switched fabric and a plurality of devices (see figure 6 of Bojinov et al.).

Referring to claim 6:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose that a file-level read request produces one or more block-level read requests (see page 3, paragraph [0030], lines 8-12 of Bojinov et al.).

Referring to claim 9:

Bojinov et al. teach:

A storage system including storage device, the storage system being coupled to a host device via a network (see e.g. figure 6, element 622 of Bojinov et al.), a method for storing encrypted data comprising:

Converting blocks of data to produce corresponding converted blocks of data, wherein a converted block of data is encrypted with cryptographic criteria (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.);

Receiving a read request to access the read data from the storage system, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.).

Referring to claim 10:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 9 above). Bojinov et al. further disclose storing the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 11:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 9 above). Bojinov et al. further disclose that the data could be non-encrypted (see page 4, paragraph [0030], last 5 lines of Bojinov et al.).

Referring to claim 12:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 9 above). Bojinov et al. further disclose that the system supports data encryption and data decryption (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.), and that the system supports different type of encryption method (see page 3, paragraph [0025], lines 16-19 of Bojinov et al.).

Referring to claim 13:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 9 above). Bojinov et al. further disclose accessing read data from the storage device in response to a read request, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.).

Referring to claim 14:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 9 above). Bojinov et al. further disclose storing the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data

being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 15:

Bojinov et al. teach:

A storage system comprising:

A storage component (see figure 1, element 121 of Bojinov et al.);

A cryptographic component in data communication and operable to convert blocks of data to produce the corresponding converted blocks of data (see page 1, paragraph [0014], lines 1-3 of Bojinov et al.),

Wherein the cryptographic component is further operable to receive read and write request for data stored on the storage component and convert the data blocks (see page 1, paragraph [0012], lines 7-9 of Bojinov et al.),

Wherein the cryptographic component is further operable to access the read data from the storage device in response to a read request, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.),

Wherein the cryptographic component is further operable to store the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 16:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 15 above). Bojinov et al. further disclose a file system configured to receive file-level read and write requests from one or more host devices, to produce the read and write requests based on the file-level read and write requests, and to communicate the read and write requests to the cryptographic component (see page 2, paragraph [0019], lines 6-9 of Bojinov et al.).

Referring to claim 17:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 15 above). Bojinov et al. further disclose

the interfaces between the components in the system (see figure 1, elements 110, 120, 130 of Bojinov et al.).

Referring to claim 20:

Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 15 above). Bojinov et al. further disclose that the cryptographic process could be null, which results in non-encrypted data (see page 4, paragraph [0030], last 5 lines of Bojinov et al.).

Referring to claim 21:

Bojinov et al. teach:

A method for storing and accessing data on a storage system comprising:

Receiving requests to access the read data from the storage system (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.);

Converting blocks of data to produce corresponding converted blocks of data (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.);

Performing a decryption of the block of data to produce an unencrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.);

Performing an encryption of the block of data to produce an encrypted block of data (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.);

Overwriting the block of data (see page 2, paragraph [0021], last 4 lines of Bojinov et al.);

Receiving a read request to access the read data from the storage system, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.);

Storing the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 22:

Bojinov et al. teach the claimed subject matter: a method for storing and accessing data on a storage system (see claim 21 above). Bojinov et al. further

disclose that the steps of encryption and decryption comprise executing computer program code on a data processing component (see claims 26, 28 of Bojinov et al.).

Referring to claim 23:

Bojinov et al. teach the claimed subject matter: a method for storing and accessing data on a storage system (see claim 21 above). Bojinov et al. further disclose a communication network comprising a switched fabric and a plurality of devices (see figure 6, elements 610, 620, 622, 624 of Bojinov et al.).

Referring to claim 25:

Bojinov et al. teach the claimed subject matter: a method for storing and accessing data on a storage system (see claim 21 above). Bojinov et al. further disclose that the data are typically stored in a manner that may be physically and/or logically sequential (see page 2, paragraph [0018], lines 1-2 of Bojinov et al.).

Referring to claim 27:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose storing the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Referring to claim 28:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose the data storage supports file-level write request (see page 2, paragraph [0019], lines 6-9 of Bojinov et al.), which produces block-level write requests (see page 3, paragraph [0030], lines 8-12 of Bojinov et al.).

Referring to claim 29:

Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). Bojinov et al. further disclose a host device (see e.g. figure 1, element 622 of Bojinov et al.).

Referring to claim 30:

Bojinov et al. teach:

A method for storing encrypted data comprising:

Converting blocks of data to produce corresponding converted blocks of data, wherein a converted block of data is encrypted with cryptographic criteria (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.);

Receiving a read request to access the read data from the storage system, decrypting the read data using the cryptographic criteria to produce the decrypted block of data (see page 1, paragraph [0014], lines 5-8 of Bojinov et al.).

Referring to claim 31:

Bojinov et al. teach the claimed subject matter: method for storing encrypted data (see claim 30 above). Bojinov et al. further disclose overwriting the block of data (see page 2, paragraph [0021], last 4 lines of Bojinov et al.).

Referring to claim 32:

Bojinov et al. teach the claimed subject matter: method for storing encrypted data (see claim 30 above). Bojinov et al. further disclose storing the data block to the storage device in response to a write request from the host device, and encrypting the data block with the cryptographic criteria before the data being written to the data storage (see page 3, paragraph [0025], lines 10-16 of Bojinov et al.).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bojinov et al. (U.S. Pub. No. 2005/0102498), and further in view of Ashton (U.S. Pub. No. 2004/0125077).

Referring to claim 5:

i. Bojinov et al. teach the claimed subject matter: a method for encrypted data storage in a storage system (see claim 1 above). However, Bojinov et al. do not specifically mention that encrypting and decrypting are performed on the logic circuitry.

ii. Ashton discloses a method wherein a logic circuit includes circuitry and/or program instructions for decryption, encryption, or data comparison (see page 4, paragraph [0040], lines 9-11 of Ashton).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ashton into the method of Bojinov et al. to perform encrypting and decrypting on a logic circuitry.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Ashton into the system of Bojinov et al. to perform encryption and decrypting on the logic circuitry, because the logic circuitry can be configured to manage data operations, and can act as a gateway limiting data that can be written to writeable memory, and processing data read from writeable memory or read only memory (see page 4, paragraph [0040], lines 3-6 of Ashton).

Referring to claim 24:

i. Bojinov et al. teach the claimed subject matter: a method for storing and accessing data on a storage system (see claim 21 above). However, Bojinov et al. do not specifically mention that encrypting and decrypting are performed on the logic circuitry.

ii. Ashton discloses a method wherein a logic circuit includes circuitry and/or program instructions for decryption, encryption, or data comparison (see page 4, paragraph [0040], lines 9-11 of Ashton).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ashton into the method of Bojinov et al. to perform encrypting and decrypting on a logic circuitry.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Ashton into the system of Bojinov et al. to perform encryption and decrypting on the logic circuitry, because the logic circuitry can be configured to manage data operations, and can act as a gateway limiting data that can be written to writeable memory, and processing data read from writeable memory or read only memory (see page 4, paragraph [0040], lines 3-6 of Ashton).

5. Claims 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bojinov et al. (U.S. Pub. No. 2005/0102498), and further in view of Cane et al. (U.S. Pattern No. 5,940,507).

Referring to claim 18:

i. Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 15 above). However, Bojinov et al. do not specifically mention that the cryptographic component comprises one or more encryption engines.

ii. Cane et al. disclose a system wherein a cryptographic engine is utilized to encrypt a file (see figure 1, element 14; and column 3, lines 45-47 of Cane et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cane et al. into the system of Bojinov et al. to utilize one or more encryption engines to perform encrypting.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cane et al. into the system of Bojinov et al. to utilize encryption engines, because an encryption engine may invoke a specialized encryption hardware

to do the encrypting, depending on the encryption method desired (see column 3, lines 51-55 of Cane et al.), thus it is more efficient.

Referring to claim 19:

i. Bojinov et al. teach the claimed subject matter: a system for encrypted data storage in a storage system (see claim 15 above). However, Bojinov et al. do not specifically mention that the cryptographic component is operable to obtain the criteria which specify the cryptographic process.

ii. Cane et al. disclose a system wherein the cryptographic component is operable to obtain the cryptographic criteria (see figure 1, elements 18, 22 of Cane et al.).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Cane et al. into the system of Bojinov et al. to make the cryptographic component to be operable to obtain the cryptographic criteria.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Cane et al. into the system of Bojinov et al. to make the cryptographic component to be operable to obtain the cryptographic criteria, because the cryptographic component supports various encryption methods (see column 3, lines 51-55 of Cane et al.), thus it is advantageous to let the application specify the desired cryptographic criteria and send them to the cryptographic component.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan
August 11, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100